Ремизов Дмитрий Владимирович, аспирант
Научный руководитель: Астрецов Дмитрий Вячеславович, проф., канд. техн. наук

ОБЗОР НЕКОТОРЫХ МЕТОДОВ УТЕЧКИ ИНФОРМАЦИИ С ПЕРСОНАЛЬНЫХ КОМПЬЮТЕРОВ

Под техническими каналами утечки информации понимают совокупность объекта разведки, с помощью которого добывается информация об этом объекте, и физической среды, в которой распространяется информационный сигнал. По сути под техническим каналом утечки информации понимают способ получения с помощью технического средства разведки информации об объекте.

Сигналы являются материальными носителями информации. По своей физической природе сигналы могут быть электрическими, электромагнитными, акустическими и т.д., то есть сигналами, как правило, являются электромагнитные, механические и другие виды колебаний (волн), причем информация содержится в изменяющихся параметрах, которая может представлять собой:

- речь
- изображение
- файлы в памяти ЭВМ и т.д.

В воздушных каналах утечки информации средой распространения акустических сигналов является воздух, и для их перехвата используются миниатюрные микрофоны.

Высокочастотное навязывание - один из эффективных способов извлечения информации из устройств, при котором происходит зондирование носителя информации высокочастотными сигналами и прием отраженных сигналов. Если падающий сигнал попадает на нелинейный элемент, то отраженный получает модуляцию. На приемной стороне выделяется одна из гармоник и производится выделение полезной составляющей. Принятый сигнал будет иметь малоиндексную амплитудно-фазовую модуляцию.

Одним из каналов утечки изображения является излучение мониторов, которое можно принять, обработать и вывести на материальный носитель.

Это направление по защите информации исследуется уже более двадцати лет [1]. Одним из средств борьбы является применение помех. Показано, что наилучшей помехой, препятствующей утечке информации, является сигналоподобная помеха [2].

Но эти помехи не эффективны в случае приема информации в оптической области частот [3]. Интенсивность света, излучаемого при развертке экрана как функция времени, соответствует свертке видеосигнала с импульсной характеристикой люминофоров. Эксперименты с типичным цветным монитором персонального компьютера показали, что в излучаемом свете остается достаточно высокочастотных составляющих, чтобы дать возможность для получения читаемого текста из восстановленного сигнала методом обращения (разделения) свертки, полученного фоточувствительным элементом. Эта потеря защищенной информации может происходить даже после рассеянного отражения от

стены. Флуктуационный шум от фонового света является важным фактором, влияющим на работоспособность такой системы. В достаточно темном помещении и с достаточно большой апертурой чувствительного элемента возможен прием на значительных расстояниях.

Светодиодные индикаторы состояния на аппаратуре передачи данных при некоторых условиях тоже могут служить источником утечки информации, при этом они несут модулированный оптический сигнал, который является коррелированным с информацией, обрабатываемой устройством. Физический доступ не требуется - злоумышленник получает доступ ко всем данным, проходящим через устройство, включая открытый текст даже в случае систем шифрования данных. Эксперименты показали, что возможно считывание информации на расстоянии до 10-15 метров от источника [4].

Таким образом, при разработке систем безопасности необходим комплексный подход, учитывающий множество факторов, но при этом возрастает стоимость мер защиты. Необходимо найти компромисс, чтобы стоимость защищаемой информации не оказалась меньшей, чем средства по ее защите.

Библиографический список

1. Wim van Eck: "Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?", Computers & Security, Vol. 4, pp. 269–286, 1985.
2. Вострецова Е.В., Нифонтов Ю.А. Оптимизация помех, затрудняющих распознавание сигналов //Автоматика и информационные технологии", серия "Научные школы УГТУ-УПИ": Сборник. 1999. №5.
3. Markus G. Kuhn Optical Time-Domain Eavesdropping Risks of CRT Displays Proceedings 2002 IEEE Symposium on Security and Privacy,12–15 May 2002, Berkeley, California, pp. 3–18
4. Joe Loughry, David A. Umphress Information Leakage from Optical Emanations ACM Transactions on Information and System Security, Vol. 5, No. 3, August 2002, pp. 262–289.